Також важливу роль у впроваджені цифрових технологій в галузі будівництва відіграють програмні комплекси, за допомогою яких розраховується вартість будівництва. Листом Міністерства регіонального розвитку та будівництва України визначено перелік рекомендованих програмних комплексів для визначення вартості будівництва [3]. За допомогою них здійснюється розрахунок вартості будівництва згідно діючих норм та правил. З їх появою процес розрахунку вартості будівництва значно прискорився.

Однією з важливих проблем, яка потребує вирішення в т.ч. впровадженням цифрових технологій є удосконалення критеріїв для визначення переможців тендерних державних закупівель. Поки основним критерієм для визначення переможця тендерних торгів вважається найнижча запропонована вартість роботи чи послуги. Проте це далеко не завжди запорука вчасного та якісного виконання робіт – швидше навпаки. Тому, на нашу думку, важливим є впровадження інших критеріїв відбору. Визначення цих критерії та їх інтеграція в існуючі цифрові технології потребує детальних досліджень результатом яких має бути внесення відповідних змін в діючі нормативно-правові документи.

Також важливою залишається проблема унормованості критеріїв для визначення граничних вартостей матеріалів, які використовуються для виконання будівельних робіт за кошти державного чи місцевих бюджетів. Діючі на даний момент норми не в повній мірі цей аспект відображають, завдяки чому існують подвійні трактування деяких позицій норм. На нашу думку, існує необхідність розробки єдиної бази формування цін на матеріали, яка дасть змогу вирішити дану проблему. Звичайно, формування такої бази даних має здійснюватись за допомогою цифрових технологій.

Для вирішення вищезгаданих проблем, а також для удосконалення існуючих цифрових технологій в галузі будівництва, на нашу думку, необхідно розглянути можливість залучення штучного інтелекту, зважаючи на досить серйозний рівень його розвитку.

Висновки. Проаналізовано основні існуючі цифрові технології, які використовуються для державного регулювання галузі будівництва та розглянуто проблеми галузі будівництва. Визначено напрямки вдосконалення критеріїв системи відбору для визначення переможця тендерних торгів та необхідність розробки єдиної бази формування цін на матеріали, що крім законодавчих змін потребує впровадженням нових цифрових рішень.

Це сприятиме удосконаленню системи державного регулювання галузі будівництва України та посилення контролю над використанням бюджетних коштів.

Список використаних джерел

1. Про внесення змін до деяких законодавчих актів України щодо удосконалення порядку надання адміністративних послуг у сфері будівництва та створення Єдиної державної електронної системи у сфері будівництва. Закон України від 17 жовтня 2019 року № 199-IX. Дата оновлення 10 жовтня 2022 року. URL : https://zakon.rada.gov.ua/laws/show/199-20#Text (дата звернення 09 листопада 2024 року).
2. Про публічні закупівлі. Закон України від 25 грудня 2015 року № 922-VIII. Дата оновлення 23 жовтня 2024 року. URL : https://zakon.rada.gov.ua/laws/show/922-19#Text (дата звернення 09 листопада 2024 року).
3. Про програмні комплекси з визначення вартості будівництва. Лист Міністерства регіонального розвитку та будівництва України від 26 грудня 2008 року № 9/5-1279. URL : https://zakon.rada.gov.ua/rada/show/v1279661-08#Text (дата звернення 09 листопада 2024 року).

ПАВЛЕНКО *І.М.*
Сумський *ОІППО*

ІНФОРМАЦІЙНА БЕЗПЕКА УЧАСНИКІВ ОСВІТНЬОГО ПРОЦЕСУ

Анотація: *У статті розглядається питання інформаційної безпеки в контексті сучасного освітнього процесу. Проаналізовано широкий спектр загроз, таких як кібератаки, витік персональних даних, несанкціонований доступ до інформаційних ресурсів тощо. Пропонуються рекомендації щодо впровадження ефективних систем захисту інформації в освітніх закладах.*

Ключові слова: інформаційна безпека, освітній процес, інформаційні загрози.

Сьогодні в умовах стрімкого розвитку інформаційних технологій, формування цифрових навичок набуває особливого значення. Вміння використовувати цифрові технології в навчанні та подальшій роботі стає необхідним для більшості професій [2]. Завдяки онлайн-навчанню здобувачі освіти отримують більш широкі можливості для здобуття знань, умінь, навичок у багатьох сферах та опануванню необхідних компетентностей. В інформаційному суспільстві соціальні мережі відкривають користувачам безмежні можливості й стають важливим інструментом масової та публічної комунікації, головна особливість якої – інтерактивність. Соціальні мережі сприяють захопленню високими технологіями, стимулюють самостійну пізнавальну діяльність, підштовхують до саморозвитку. Але останнім часом вони містять чимало небезпек: стали осередком фейкових новин, кризи інформації та психологічної залежності. Академічна прокрастинація – психологічна проблема більшості здобувачів освіти. Здобувачі освіти, які перебувають в умовах постійної психологічної напруги схильні відкладати справи на потім, що призводить до виконання їх при жорсткому дефіциті часу. Це позначається не тільки на якості, успішності навчання, а й на психофізіологічному стані учня, на його особистості загалом. Користувачі комп'ютера також схильні до адикції: вони знаходяться у своєрідному психологічному трансі, в якому реальність набуває не чітких рис і зливається з віртуальністю, що сприяє несвідомому засвоєнню інформації [3]. Аудіо-візуальна інформація найбільш приваблива й легка для сприйняття широкому колу користувачів соціальних мереж, яка використовуються для маніпуляції: пости у Facebook та на каналах Telegram, відеоматеріали на YouTube та Instagram; фейкових повідомлення в Інтернет месенджерах Viber/WhatsApp/Telegram, вірусні SMS; ефірні та Інтернет-передачі; масові розсилки на адреси електронної пошти. Також, останніми роками суб'єкти маніпулювання суспільною свідомістю створюють псевдокористувачів соцмереж, так звані ботоферми, та від їх імені пишуть тисячі коментарів. Реалізаторами маніпулятивних технологій також можуть бути реальні люди, які просувають певну інформацію в інтернет-просторі, так звані «ломи» (лідери суспільної думки). Це, здебільшого, блогери, які мають велику кількість підписників, авторитети, до думки яких дослухаються, а їхні дописи поширюють у мас-медіа [4]. Захищеність здобувачів освіти від вище перелічених небезпек у соціальних мережах, які зможуть спричинити деструктивний вплив на їхню свідомість, є досить важливим завданням педагогічних працівників закладів освіти. Питання інформаційної безпеки набувають особливого значення в умовах кризи, ведення війни, саме тоді, коли здатність чинити опір послаблена завдяки страху, паніки, дезорієнтації. Саме тому важливо дотримуватися базових правил інформаційної гігієни [5] і бути особливо пильними до інформації, що надходить і яка поширюється. А молодь потребує особливого захисту, адже саме від її розвитку залежить майбутнє країни.

Наразі, дуже важливо створювати умови для підняття рівня критичного мислення у здобувачів освіти: вирізняти офіційні джерела інформації, сумніватися, уміти перевіряти інформацію, щоб розпізнавати фейки, аналізувати різні точки зору, розрізняти переконливі аргументи та прояви маніпуляції.

Аналіз закордонних та вітчизняних літературних джерел з питань інформаційної безпеки дозволяє стверджувати, що вчені вважають її складовою інформаційної культури особистості (І. Теплицький, С. Семеріков та ін.). Питання формування інформаційної культури вчителя висвітлено в працях В. Бикова, О. Данильчука, М. Жалдака, А. Коломієць, Л. Гаврілової.

Серед українських учених значну увагу питанням інформаційної безпеки приділяють такі вчені, як Р. Калюжний, Г. Почепцов, Б. Кормич, П. Жарков. Іноземні публікації представлені такими авторами як І. Панарів, А. Тер-Акопов, В. Ярчкин.

Так, М. Жалдак, наголошуючи на необхідності використання комп'ютерної техніки та засобів зв'язку, стверджує, що таке користування має бути педагогічно виваженим і доцільним.

Метою статті є дослідження і аналіз поняття «інформаційна безпека» різними вченими і практиками, розробка практичних рекомендацій для всіх учасників освітнього процесу щодо безпеки в кіберпросторі.

Початок третього тисячоліття ознаменовано народженням суспільства нового типу − інформаційного, в якому основним стратегічним ресурсом постає інформація. Вплив, який чинять інформаційні процеси на всі сфери державного та суспільного життя, актуалізує найважливіші питання соціального буття, в тому числі питання інформаційних взаємодій, включаючи боротьбу за інформаційний простір і протидія різного роду інформаційним загрозам [1].

Приблизно 82% українців користуються Інтернетом хоча б раз на тиждень, із них 78% щодня чи майже щодня [4]. Тому і набуває гостроти питання інформаційної безпеки.

Інформаційна безпека стосується захисту життєво важливих інтересів людини (і більш глобально – суспільства, держави). Неправдива, неповна, невчасна інформація може нанести шкоду. Нині, коли на території України ведуться повномасштабні бої, війна триває і в Інтернеті. У складні для нашої країни часи важливо захищати себе не лише фізично, а й інформаційно.

Роль інформаційної сфери, яка представляє собою сукупність інформації, інформаційної інфраструктури суб'єктів, які здійснюють збір, формування, поширення і використання інформації, а також систем регулювання виникаючих при цьому громадських відносин, значно зросла на сучасному етапі розвитку суспільства.

Одним зі шляхів забезпечення інформаційної безпеки здобувачів освіти є організація безпечного особистісного інформаційного простору як у школі, так і в сім'ї. Організувати безпечний інформаційний простір можливо шляхом реалізації засобів та заходів щодо інформаційної безпеки здобувачів освіти, серед яких: правові, технічні та програмні, виховні й організаційні, моральні й етичні.

Забезпечення інформаційної безпеки та кібербезпеки здобувачі освітив в умовах воєнного стану є надзвичайно важливим завданням. Педагогічні колективи продовжують впевнено тримати свій освітній фронт у важких умовах війни, набувають унікального педагогічного досвіду, перебувають у постійному пошуку нових освітніх підходів, ефективних педагогічних й інформаційних технологій та беруть на себе новий рівень відповідальності за майбутнє країни. Освітній процес зазнав змін не лише в змісті й формах освіти, а й в умовах організації з огляду на безпекову ситуацію.

У разі збереження можливості надання закладом освітніх послуг та враховуючи реалії українського сьогодення, кожен учасник освітнього процесу має володіти інформацією щодо захисту життя і здоров'я та докладати максимум зусиль для створення безпечного середовища як в умовах воєнного стану, так і в будь який інший період.

Для забезпечення безпеки дітей і дорослих великого значення має інформаційна безпека. Батьки та педагоги можуть самі регулювати потік інформації, що надходить до них. Але здобувачі освіти шкільного віку цього робити не завжди можуть, проте, в період воєнного часу, вони майже постійно перебувають в інформаційно-стресовому полі. Саме тому надзвичайно важливо навчити шкільну спільноту відповідально і свідомо споживати інформацію так, щоб не наразити себе та інших на небезпеку, не стати жертвою обману, відділити корисну інформацію від непотрібної чи шкідливої.

Провідну роль у недопущенні доступу здобувачів освіти до матеріалів, несумісних із завданнями навчання, особливо за переважної відсутності контент-фільтруючих програм у школі і вдома, є навчання і виховання з метою формування інформаційно безпечної особистості.

Інформацію слід подавати відповідно до віку та дбати, щоб вона її не травмувала. Здобувачі освіти мають право знати, що відбувається в їхній країні, але дорослі також мають відповідальність убезпечити дітей від небезпечного контенту.

Онлайн-безпека в інформаційному суспільстві є одним з основних напрямів фундаментальних досліджень у сфері інформаційних технологій, які використовуються під час вивчення практично всіх шкільних дисциплін уже з початкової школи.

Визначають такі види кіберзагроз:

- загрози для особистісної безпеки: загроза ознайомлення з матеріалами небажаного змісту (порнографія, ненормативна лексика, публікації суїцидального характеру, сектантські, расистські та ненависницькі матеріали, щодо створення вибухових речовин, хакерські сайти); загроза отримання недостовірної інформації; Інтернет-залежність; загроза спілкування з небезпечними людьми (шахраями, збоченцями, гриферами тощо); загрози вчинення протиправних дій (хакерство, порушення авторських прав тощо);
- загрози витоку персональної інформації: загроза розголошення персональних і корпоративних даних (прізвища, імені, адреси, номери банківських карток, телефонів тощо).
- загрози для персональних комп'ютерів: загроза комп'ютерних вірусів; загроза завантаження шкідливого активного коду тощо.

Сучасні технології кібербезпеки освітнього процесу передбачають забезпечення захисту на 5-ти рівнях: нормативно-правовий; морально-етичний; адміністративно-організаційний; фізичний і технічний.

Проведено класифікацію найпоширеніших кіберзагроз у секторі освіти. З'ясовано, що людський фактор, тобто помилки співробітників або здобувачів освіти внаслідок необізнаності або зневажання елементарними правилами кібергігієни лежать в основі більшості успішно реалізованих

кібератак. Дослідження ознак кіберзагроз у галузі освіти надав можливість розділили їх за дев'ятьма критеріями: загрози на пристрої IoT (система взаємопов'язаних комп'ютерних пристроїв, які наділені унікальними ідентифікаторами та здатні передавати дані через мережу без вимоги взаємодії між людьми та комп'ютерами), загрози через людський фактор, крадіжка персональних даних, програми-вимагачі або зловмисне програмне забезпечення, фінансова вигода, шпигунство, фішинг, DDoS-атаки (атаки на відмову в обслуговуванні та спрямовані на веб-сайти й сервери та здійснюються для того, щоб порушити роботу мережевих служб, загрози на CMS (кібератаки на веб-сайти) [3].

Щоб не стати жертвою кібератак, необхідно дотримуватися певних рекомендацій під час роботи у мережі Інтернет усім учасникам освітнього процесу.

Для безпечної роботи в кіберпросторі педагогам рекомендуємо:

- Не користуйтесь забороненим и поштовими сервісами (Mail.ru, Yandex) та соціальним мережами (Vkontakte, Одноклассники).
- Використовуйте антивірусні програми.
- Користуйтесь надійними паролями, періодично змінюйте їх.
- Оновлюйте програмне забезпечення.
- Залучайте батьків до профілактичної роботи з дітьми, проводьте бесіди для батьків щодо проблем кіберзагроз та засобів їх упередження.
- Використовуйте систему превентивних заходів для вирішення проблеми кіберзахисту в шкільному середовищі.
- Використовуйте активні та інтерактивні форми роботи, такі як: перегляд кінострічок, роликів на тему кібербезпеки, обговорення переглянутого, моделювання ситуацій, які схожі на ті, які реально відбуваються, та пошуки виходу з них.
- Проводьте діагностику стану психологічного клімату класу, виявляйте дітей, які зазнавали віртуального цькування або можуть піддаватися кібербулінгу. [6].

Отже, сучасний учитель повинен знати основні напрями кібербезпеки в Україні та світі, принципи безпеки цифрових технологій у професійній діяльності, засоби забезпечення кібербезпеки системи освіти; уміти безпечно використовувати ресурси інформаційних освітніх систем; інтегрувати засоби кібербезпеки, сучасні інформаційні технології в освітню діяльність; користуватися засобами кібербезпеки електронних освітніх ресурсів для навчання з урахуванням психолого-педагогічних особливостей здобувачі освітив. І, окрім того, інформаційна безпека в умовах становлення глобального інформаційного суспільства тісно пов'язана з проблемами забезпечення безпеки особистості, а також соціуму в цілому.

Список використаних джерел

1. Доценко С. О. Онлайн-безпека учасників освітнього процесу в умовах дистанційного і змішаного навчання : навч.-метод. посіб. / С. О. Доценко, В. В. Ворожбіт-Горбатюк, Т. М. Собченко. Харків : Вид-во «Ранок». 2021. 192 с.
2. Жадан І. Інформаційна безпека середовища як чинник розвитку громадянської компетентності молоді. Проблеми політичної психології. 24(1), 248-257. URL: https://doi.org/10.33120/popp-Vol24-Year2021-77 (дата звернення: 29.10.2024).
3. Золотар О.О. Інформаційна безпека людини : теорія і практика : монографія. Київ : ТОВ «Видавничий дім «АртЕк», 2018. 446 с.
4. Користування Інтернетом серед українців: результати опитування, проведеного 13-18 травня 2022 року. Київський міжнародний інститут соціології URL : https://www.kiis.com.ua/?lang=ukr&cat=reports&id=1115& page =1 (дата звернення: 29.10.2024).
5. Кормич Б.А. Інформаційна безпека: організаційно-правові основи: Навч.посібник. К. : Кондор, 2004. 384 с.
6. Косенчук О., Стягунова О. Безпека освітнього простору в закладах дошкільної освіти в умовах воєнного стану. Науковий журнал «Духовність особистості: методологія, теорія і практика», том 1 № 3 (107) (2023): Духовність особистості: методологія, теорія і практика: збірник наукових праць, 2013 С.90-101.
7. Степаненко О.І., Семеняко Ю.Б., Цапко А.М. Формування цифрових компетентностей педагога під впливом кризових ситуацій в Україні. *Академічні студії. Серія* «*Педагогіка*». 2022. Вип. 2. С. 92-98.